LMS J. Comput. Math. 18 (1) (2015) 684–698
doi:10.1112/S1461157015000224

On λ-invariants attached to cyclic cubic number fields

Daniel Delbourgo and Qin Chao

Abstract

We describe an algorithm for finding the coefficients of $F(X)$ modulo powers of p, where $p \neq 2$ is a prime number and $F(X)$ is the power series associated to the zeta function of Kubota and Leopoldt. We next calculate the 5-adic and 7-adic λ-invariants attached to those cubic extensions $K/\mathbb{Q}$ with cyclic Galois group $\mathcal{A}_3$ (up to field discriminant $<10^7$), and also tabulate the class number of $K(e^{2\pi i/p})$ for $p = 5$ and $p = 7$. If the λ-invariant is greater than zero, we then determine all the zeros for the corresponding branches of the p-adic L-function and deduce Λ-monogeneity for the class group tower over the cyclotomic $\mathbb{Z}_p$-extension of K.

Supplementary materials are available with this article.

1. *Introduction*

The connection between arithmetic invariants of number fields and special values of L-functions has proven to be a rich theme in algebraic number theory. The first hint that this link may have a p-adic formulation can be found in the work of Kummer in the 19th century, and this connection was subsequently greatly developed by Kenkichi Iwasawa in the mid-20th century. In more recent times Coates, Wiles, Mazur, Greenberg, Perrin-Riou and many others, have extended Iwasawa's fundamental ideas to a general motivic setting. It is now widely seen that there should be a precise correlation between certain Iwasawa-theoretic invariants $\mu, \lambda \geqslant 0$, attached to the arithmetic object over the cyclotomic $\mathbb{Z}_p$-extension and the nature of the finite number of zeros (and the leading term) in its associated p-adic L-function.

This paper reports on a modest computational project to find the zeros of the p-adic L-functions attached to cubic number fields. The calculation of the zeros over $\mathbb{Q}$ was initiated by Wagstaff [**16**, **17**] in the late nineteen-seventies, and developed by Childress and Gold [**1**]; the various methods were extended to quadratic fields in the work of Ernvall and Metsänkylä [**5**, **6**] a decade or so later. Of course, the Iwasawa Main Conjecture (proved by Mazur and Wiles [**13**, **19**]) relates these zeros to the Λ-module structure of certain towers of ideal class groups. Recently Ellenberg, Jain and Venkatesh [**4**] have studied the connection between the way in which the number of zeros varies over a family of quadratic fields and the statistics predicted by the corresponding p-adic random matrices. One therefore expects that the techniques developed here can be used to study an analogous problem for a family of cubic twists instead.

Let K be a cyclic cubic field of discriminant D_K. We shall undertake the following tasks at both the primes 5 and 7:

(I) calculate the λ-invariant for all cyclic cubic fields K up to discriminant $D_K < 10^7$; and
(II) determine the zeros of each p-adic L-function, again for all K with $D_K < 10^7$.

The reason why we chose 10^7 as the cut-off value for the discriminant is that the tables of Llorente and Quer [**11**] terminate at this point; that leaves 501 such cyclic fields K to consider. Since the relevant p-adic L-function exhibits two non-trivial branches when $p = 5$, and three non-trivial branches when $p = 7$, this amounts to $(2 + 3) \times 501 = 2505$ different branches for which we potentially need to locate zeros.

Received 16 April 2015; revised 2 September 2015.
2010 Mathematics Subject Classification 11R23 (primary), 11M41, 11R60 (secondary).

Here is a short plan of the paper. In § 2 we give a method to approximate the Taylor series expansion of the power series associated to the p-adic L-function, modulo a topologically nilpotent ideal $\mathcal{J}_N$ in the Iwasawa algebra Λ. Then, in § 3, we focus exclusively on cyclic cubic fields K, and supply two separate methods to work out the λ-invariant for each branch. We next describe how to locate any p-adic zeros whenever the λ-invariant is strictly positive and give an irreducible polynomial with splitting field $K(\mu_p)$. Then we compute its class number. Finally, in § 4, we interpret the full tables of p-adic zeros compiled within the Appendix (available as online supplementary material from the publisher's website) in terms of the Iwasawa module, $\mathfrak{X}_{\infty,K}$, built out of a certain tower of p-primary class groups. We deduce that the latter has a monogenic Λ-structure.

The techniques we exploit here are quite different from those employed in [**1**, **4**, **6**, **16**, **17**]. The key ingredient is to utilise the p-adic approximations developed by the first author in [**2**, **3**], which seem well suited to resolving problems of type (I) and (II) (see previous page), relatively quickly. In total, the computations in this paper took approximately five months to run on PARI/GP. Although we could have computed the zeros of the p-adic L-functions to a larger p-adic accuracy, we chose an accuracy sufficient to show (in each case) that $\mathfrak{X}_{\infty,K}$ was Λ-monogenic. Likewise, in this paper, we only consider $p = 5$ and $p = 7$, but the method works for any odd prime p with appropriate modifications.

2. *An algorithm to compute the Taylor series*

Let $p \geqslant 3$ be a prime number, and let χ be a Dirichlet character of conductor $\mathfrak{f}_\chi$ coprime to p. Kubota and Leopoldt [**10**] constructed a p-adic zeta function $L_p(s, \chi)$ interpolating the values

$$L_p(1-n,\chi) = \iota_p((1-\chi\omega^{-n}(p)p^{n-1})\cdot\zeta(1-n,\chi\omega^{-n})) \tag{1}$$

at every positive integer n, where $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ is a fixed embedding of the algebraic numbers into the Tate field, and ω denotes the Teichmüller character modulo p.

Remark. If $\chi(-1) = -1$, these values above are identically zero. Throughout this paper we shall only consider the non-trivial branches $L_p(s, \chi\omega^{1+\beta})$ for which $\chi\omega^{1+\beta}(-1) = +1$. One may therefore index these branches using exactly half the congruence classes $\beta \bmod p-1$.

Let $\mathcal{O}$ be a finite extension of the p-adic integers containing the values of the character χ. By assuming that either $\beta \not\equiv -1 \pmod{p-1}$ or, instead, that $\beta \equiv -1 \pmod{p-1}$ and $\chi \neq \mathbf{1}$, Iwasawa established the existence of a power series $F_{\chi,\beta}(X) \in \mathcal{O}[\![X]\!]$ satisfying the property

$$F_{\chi,\beta}((1+p)^{-s}-1) = L_p(s,\chi\omega^{1+\beta}) \quad \text{at every } s \in \mathbb{C}_p \text{ with } |s|_p < p^{(p-2)/(p-1)}.$$

If $\beta \equiv -1 \pmod{p-1}$ and $\chi = \mathbf{1}$, the corresponding power series has a simple pole at $X = 1/(1+p) - 1$ and is analytic elsewhere: in fact $(X + p/(1+p)) \cdot F_{\chi,-1}(X) \in \mathcal{O}[\![X]\!]$ (see [**18**, § 7.2]). Applying the Weierstrass preparation theorem, for $\chi \neq \mathbf{1}$ there is a factorisation

$$F_{\chi,\beta}(X) = p^\mu \times \mathcal{U}(X) \times (X^\lambda + b_{\lambda-1}X^{\lambda-1} + \ldots + b_0),$$

where $|b_j|_p < 1$ for indices $j < \lambda$, the integer μ is greater than or equal to zero and $\mathcal{U}(X)$ is an invertible power series. Moreover the invariant μ is equal to zero by a fundamental result of Ferrero and Washington [**7**].

In order to compute the zeros of $F_{\chi,\beta}(X)$ it is enough to find the distinguished polynomial $X^\lambda + b_{\lambda-1}X^{\lambda-1} + \ldots + b_0$ to a reasonable accuracy, which in turn requires us to compute the initial coefficients occurring in the Taylor series for $F_{\chi,\beta}(X)$ about $X = 0$ (see [**4**, Proposition 5.3]). To date, the methods employed to work out these Taylor series coefficients have either

involved expanding $L_p(s, \chi\omega^{1+\beta})$ as a series in $s-1$ and then using some protracted linear algebra [1, 6], or have involved computing the algebraic values $\zeta(1-n, \chi)$ then applying interpolation [4]. Here we propose an alternative approach. For an integer N greater than or equal to one, consider the $\mathcal{O}[\![X]\!]$-ideals

$$\mathcal{J}_N = \prod_{j=1}^{N} (X^{p^{j-1}}, p) = (X, p) \cdot (X^p, p) \ldots (X^{p^{N-1}}, p).$$

As $N \to \infty$ the sequence of $\mathcal{J}_N$ tends to zero and, under the substitution $X \mapsto (1+p)^{-s} - 1$ (with $s \in \mathbb{Z}_p$), each specialisation $[\mathcal{J}_N]_{X=(1+p)^{-s}-1} = p^N\mathcal{O}$.

Aim. We give an algorithm to compute the Taylor series expansion for $F_{\chi,\beta}(X)$ modulo $\mathcal{J}_N$.

More precisely, we first replace $F_{\chi,\beta}$ by another power series $\mathcal{F}_{\chi,\beta}$. If $\beta \not\equiv -1$, then the two differ by a unit of $\mathcal{O}[\![X]\!]$; if $\beta \equiv -1$, then $\mathcal{F}_{\chi,-1}(X) = (X + p/(1+p)) \cdot F_{\chi,-1}(X)$ up to a unit again. The key step in the proof uses the new expansions for $\mathcal{F}_{\chi,\beta}((1+p)^{-s}-1)$ developed in [2, 3].

Notation.
- The symbol $\delta_{a<b}$ will represent the value 1 if $a < b$, and represent 0 otherwise.
- For a prime p, the function $\log_p(-)$ is Iwasawa's logarithm normalised so that $\log_p(p) = 0$.
- Writing $\langle u \rangle$ means projecting $u \in \mathbb{Z}_p^\times$ to the principal local units $1+p\mathbb{Z}_p$, so $u = \omega(u)\langle u \rangle$.

To describe our algorithm, we shall introduce two arithmetic functions θ_N and $\mathcal{L}_N$ below. Firstly let $\varpi \in \{1, \ldots, 2\mathfrak{f}_\chi - 1\}$ denote the multiplicative inverse of p modulo $2\mathfrak{f}_\chi$.

Definition 1. (a) For each pair $x, m \in \mathbb{N}$ with $p \nmid m$, we define $\theta_N(x,m) \in \{0, \ldots, 2\mathfrak{f}_\chi p^N - 1\}$ to be the unique element for which

$$\theta_N(x,m) \equiv m + (p\varpi)^N(x-m) \bmod 2\mathfrak{f}_\chi p^N.$$

(b) If $u \in \mathbb{Z}_p^\times$ is a p-adic unit, then $\mathcal{L}_N(u) \in \{0, \ldots, p^N - 1\}$ denotes the unique integer such that $\mathcal{L}_N(u) \equiv \log_p(u)/\log_p(1+p) \bmod p^N\mathbb{Z}_p$.

Now, to a fixed exponent N greater than or equal to one, we can associate the integer $\gamma_{N,t} = \lfloor p^{t\phi(2\mathfrak{f}_\chi)}/2\mathfrak{f}_\chi p^N \rfloor$ at every $t \in \mathbb{N}$. For each index j greater than or equal to zero, we define $\mathcal{O}$-valued coefficients

$$c_j^{(N)}(\mathcal{F}_{\chi,\beta}) := \sum_{m=1, p\nmid m}^{p^N} \binom{\mathcal{L}_N(m)}{j} \omega^\beta(m) \times \sum_{x=1}^{2\mathfrak{f}_\chi} a_x(\chi) \cdot \delta_{\theta_N(x,m) < p^{\mathcal{T}\phi(2\mathfrak{f}_\chi)} - 2\mathfrak{f}_\chi p^N \gamma_{N,\mathcal{T}}}, \qquad (2)$$

where the positive integer $\mathcal{T} = \mathcal{T}_N := \lfloor N/\phi(2\mathfrak{f}_\chi) \rfloor + 1$ and

$$a_x(\chi) = \zeta(0,\chi) + \sum_{j=1}^{x-1} \chi(j) - 2 \sum_{j=1}^{\lfloor (x-1)/2 \rfloor} \chi(j).$$

Theorem 1. *If $\mathcal{F}_{\chi,\beta}(X) \in \mathcal{O}[\![X]\!]$ is the power series corresponding to the Iwasawa function*

$$(2\omega^\beta(2)\langle 2 \rangle^{-s} - 1) \cdot L_p(s, \chi\omega^{1+\beta})$$

and assuming $p \nmid 2\mathfrak{f}_\chi\phi(\mathfrak{f}_\chi)$, *then there are congruences*

$$\mathcal{F}_{\chi,\beta}(X) \equiv \sum_{j=0}^{p^N} c_j^{(N)}(\mathcal{F}_{\chi,\beta}) \cdot X^j \bmod \mathcal{J}_N \quad \text{for each } N \geqslant 1. \tag{3}$$

The numbers $a_x(\chi)$ for $x = 1, \dots, 2\mathfrak{f}_\chi$ can be stored in an array, while $p^{\mathcal{T}\phi(2\mathfrak{f}_\chi)} - 2\mathfrak{f}_\chi p^N \gamma_{N,\mathcal{T}}$ is constant (for fixed N). Moreover, since $(p\varpi)^N$ is fixed, each calculation of $\theta_N(x,m)$ requires exactly three arithmetic operations. The only potentially time consuming quantity to work out is $\mathcal{L}_N(m)$ and this amounts to calculating the value of $\log_p(m)$ modulo $p^{N+1}\mathbb{Z}_p$, which itself takes $O((N+1)\log p)$-steps to work out.

COROLLARY 1. *Computing each* $c_j^{(N)}(\mathcal{F}_{\chi,\beta})$ *is of arithmetic complexity* $O(\mathfrak{f}_\chi + N\log p \cdot p^N)$.

We should also remark that the ideals $\mathcal{J}_N$ form decreasing neighbourhoods of zero under the Λ-adic topology, and hence the polynomial sequence $\{\sum_{j=0}^{p^N} c_j^{(N)}(\mathcal{F}_{\chi,\beta}) \cdot X^j\}_{N\geqslant 1}$ must be Cauchy. Consequently, the coefficients $c_j^{(N)}(\mathcal{F}_{\chi,\beta})$ are themselves Cauchy in N and their limit is precisely the X^j-coefficient of $\mathcal{F}_{\chi,\beta}$. It follows that Theorem 1 produces an easily programmable, purely p-adic method to find the power series associated to Kubota–Leopoldt zeta functions.

It is worthwhile comparing the efficiency of the above method with those in [**1**, **5**, **6**, **16**, **17**]. Focusing on the work of Ernvall–Metsänkylä (which is a synthesis of the preceding articles), in [**6**, §§ 5–8] they expand $L_p(s, \chi\omega^{1+\beta})$ as a power series $\sum_{i=0}^{\infty} u_i s^i$ for $s \in \mathbb{Z}_p$, and then approximate each u_i mod p^{M+1} (here M is essentially equivalent to N in our earlier notation). The method given in [**6**, § 11] requires the calculation of auxiliary terms '$R_{\nu i}$', which are $O(p^M)$ to work out; therefore our approach and their approach should produce comparable run-times.

(Of course, if one possessed an oracle which could instantly produce the complex L-values $\zeta(1-n, \chi\omega^{1+\beta})$ for a complete set of representatives $n \in \mathbb{Z}/p^M\mathbb{Z}$, the calculation of the Taylor series coefficients for $\mathcal{F}_{\chi,\beta}$ would be speeded up dramatically.)

Proof. We will write $\Omega(s)$ as a shorthand for the function $(2\omega^\beta(2)\langle 2\rangle^{-s} - 1) \times L_p(s, \chi\omega^{1+\beta})$. Since $\gcd(p, 2\mathfrak{f}_\chi\phi(\mathfrak{f}_\chi)) = 1$, from [**3**, Theorem 2.4],

$$\Omega(s) \equiv \sum_{m=1,\ p\nmid m}^{p^{t\phi(2\mathfrak{f}_\chi)}} a_m(\chi)\omega^\beta(m)\langle m\rangle^{-s} \bmod p^{t\phi(2\mathfrak{f}_\chi)} \quad \text{at every } t \geqslant 1,$$

where $\langle u\rangle^s = \exp_p(s\log_p(u))$ for any $u \in \mathbb{Z}_p^\times$ and $s \in \mathcal{O}_{\mathbb{C}_p}$. Let us further assume $p^N \leqslant p^{t\phi(2\mathfrak{f}_\chi)}$. Now the $a_m(\chi)$ are periodic with modulus $2\mathfrak{f}_\chi$ so that

$$\Omega(s) \equiv \sum_{x=1}^{2\mathfrak{f}_\chi} a_x(\chi) \sum_{\substack{m=1,\ p\nmid m \\ m\equiv x \,(\mathrm{mod}\, 2\mathfrak{f}_\chi)}}^{p^{t\phi(2\mathfrak{f}_\chi)}} \omega^\beta(m)\langle m\rangle^{-s} \equiv \sum_{x=1}^{2\mathfrak{f}_\chi} a_x(\chi) \sum_{m'=1,\ p\nmid m'}^{p^N} \sum_{\substack{m=1,\ p\nmid m \\ m\equiv x \,(\mathrm{mod}\, 2\mathfrak{f}_\chi) \\ m\equiv m' \,(\mathrm{mod}\, p^N)}}^{p^{t\phi(2\mathfrak{f}_\chi)}} \omega^\beta(m')\langle m'\rangle^{-s}$$

modulo p^N, since $\omega^\beta(m)\langle m\rangle^{-s} \equiv \omega^\beta(m')\langle m'\rangle^{-s}$ mod p^N.

The twin congruences $m \equiv x$ mod $2\mathfrak{f}_\chi$ and $m \equiv m'$ mod p^N can be combined together into a single congruence $m \equiv m' + (p\varpi)^N(x - m')$ mod $2\mathfrak{f}_\chi p^N$, and hence

$$\Omega(s) \equiv \sum_{m'=1,\ p\nmid m'}^{p^N} \omega^\beta(m')\langle m'\rangle^{-s} \times \sum_{x=1}^{2\mathfrak{f}_\chi} a_x(\chi) \cdot \#\mathcal{S}^{(x,m')} \bmod p^N, \tag{4}$$

where $\mathcal{S}^{(x,m')} = \{m \in \mathbb{Z} \mid 1 \leqslant m \leqslant p^{t\phi(2\mathfrak{f}_\chi)} \text{ and } m \equiv m' + (p\varpi)^N(x - m') \bmod 2\mathfrak{f}_\chi p^N\}$.

REMARKS. (i) In general, for any $\vartheta \in \{1, \dots, 2\mathfrak{f}_\chi p^N - 1\}$ with $p \nmid \vartheta$, one can consider the set

$$\mathcal{S}(\vartheta) = \{m \in \mathbb{Z} \mid 1 \leqslant m \leqslant p^{t\phi(2\mathfrak{f}_\chi)} \text{ and } m \equiv \vartheta \bmod 2\mathfrak{f}_\chi p^N\}.$$

If we divide the interval $[1, p^{t\phi(2\mathfrak{f}_\chi)}] \cap \mathbb{N}$ into $\gamma_{N,t} = \lfloor p^{t\phi(2\mathfrak{f}_\chi)}/2\mathfrak{f}_\chi p^N \rfloor$ uniform chunks of length $2\mathfrak{f}_\chi p^N$, then each full-length chunk contains exactly one solution; therefore $\#\mathcal{S}(\vartheta) = \gamma_{N,t} + \#\mathcal{S}^\dagger(\vartheta)$, where $\mathcal{S}^\dagger(\vartheta) = \{m \in \mathbb{Z} \mid 2\mathfrak{f}_\chi p^N \gamma_{N,t} \leqslant m \leqslant p^{t\phi(2\mathfrak{f}_\chi)} \text{ and } m \equiv \vartheta \bmod 2\mathfrak{f}_\chi p^N\}$.

(ii) To determine the size of $\mathcal{S}^\dagger(\vartheta)$, we need only observe that $\#\mathcal{S}^\dagger(\vartheta)$ will be one or zero, depending upon whether or not $\vartheta + 2\mathfrak{f}_\chi p^N \times \gamma_{N,t}$ is strictly less than the end point $p^{t\phi(2\mathfrak{f}_\chi)}$. One therefore concludes that

$$\#\mathcal{S}(\vartheta) = \gamma_{N,t} + \begin{cases} 1 & \text{if } \vartheta < p^{t\phi(2\mathfrak{f}_\chi)} - 2\mathfrak{f}_\chi p^N \gamma_{N,t}, \\ 0 & \text{otherwise,} \end{cases} = \gamma_{N,t} + \delta_{\vartheta < p^{t\phi(2\mathfrak{f}_\chi)} - 2\mathfrak{f}_\chi p^N \gamma_{N,t}}.$$

(iii) As a special case, $\#\mathcal{S}^{(x,m')} = \gamma_{N,t} + \delta_{\theta_N(x,m') < p^{t\phi(2\mathfrak{f}_\chi)} - 2\mathfrak{f}_\chi p^N \gamma_{N,t}}$ (see Definition 1(a)).

Substituting our expression for $\#\mathcal{S}^{(x,m')}$ back into equation (4), one obtains

$$\Omega(s) \equiv \sum_{m'=1,\ p\nmid m'}^{p^N} \omega^\beta(m')\langle m'\rangle^{-s} \times \sum_{x=1}^{2\mathfrak{f}_\chi} a_x(\chi) \cdot (\gamma_{N,t} + \delta_{\theta_N(x,m') < p^{t\phi(2\mathfrak{f}_\chi)} - 2\mathfrak{f}_\chi p^N \gamma_{N,t}}) \bmod p^N$$

and as the sum of the $a_x(\chi)$ always equals zero, this simplifies further to become

$$\Omega(s) \equiv \sum_{m=1, p\nmid m}^{p^N} \omega^\beta(m)\langle m\rangle^{-s} \times \sum_{x=1}^{2\mathfrak{f}_\chi} a_x(\chi) \cdot \delta_{\theta_N(x,m) < p^{t\phi(2\mathfrak{f}_\chi)} - 2\mathfrak{f}_\chi p^N \gamma_{N,t}} \bmod p^N. \tag{5}$$

Before completing the proof of Theorem 1, observe that, under the transformation $X \mapsto (1+p)^{-s} - 1$, the power series representing $\langle m\rangle^{-s}$ is given by expanding $(1+X)^{\log_p(m)/\log_p(1+p)}$ in terms of X. Using Definition 1(b) one finds that $(1+X)^{\log_p(m)/\log_p(1+p)} \equiv (1+X)^{\mathcal{L}_N(m)} \bmod ((1+X)^{p^N} - 1) \cdot \mathcal{O}[\![X]\!]$. Furthermore,

$$(1+X)^{p^N} - 1 = X \cdot \prod_{j=1}^{N} \frac{(1+X)^{p^j} - 1}{(1+X)^{p^{j-1}} - 1} = (X^p + O(pX)) \cdot \prod_{j=2}^{N} (X^{p^{j-1}} + O(X^{p^{j-1}+1}) + O(p)),$$

which lies in the ideal $\widetilde{\mathcal{J}_N} = (X^p, pX) \cdot (X^p, p) \cdot (X^{p^2}, p) \dots (X^{p^{N-1}}, p)$ of the Iwasawa algebra; the inclusion $(X^p, pX) \subset (X, p)$ then implies this latter ideal $\widetilde{\mathcal{J}_N} \subset \mathcal{J}_N$.

NOTATION. To ease congestion, we now abbreviate $\delta_{\theta_N(x,m) < p^{t\phi(2\mathfrak{f}_\chi)} - 2\mathfrak{f}_\chi p^N \gamma_{N,t}}$ simply to δ_{θ_N}.

Recalling that $\Omega(s) = \mathcal{F}_{\chi,\beta}((1+p)^{-s} - 1)$, the congruence (5) yields the weaker version

$$\mathcal{F}_{\chi,\beta}(X) \equiv \sum_{m=1,\ p\nmid m}^{p^N} \omega^\beta(m)(1+X)^{\mathcal{L}_N(m)} \times \sum_{x=1}^{2\mathfrak{f}_\chi} a_x(\chi) \cdot \delta_{\theta_N} \bmod \mathcal{J}_N.$$

The binomial theorem tells us that $(1+X)^{\mathcal{L}_N(m)} = \sum_{j=0}^{p^N} \delta_{j \leqslant \mathcal{L}_N(m)} \binom{\mathcal{L}_N(m)}{j} X^j$, and hence

$$\begin{aligned} \mathcal{F}_{\chi,\beta}(X) &\equiv \sum_{m=1,\ p\nmid m}^{p^N} \omega^\beta(m) \times \sum_{x=1}^{2\mathfrak{f}_\chi} a_x(\chi) \cdot \delta_{\theta_N} \sum_{j=0}^{p^N} \delta_{j \leqslant \mathcal{L}_N(m)} \binom{\mathcal{L}_N(m)}{j} X^j \\ &\equiv \sum_{j=0}^{p^N} X^j \times \left(\sum_{m=1,\ p\nmid m}^{p^N} \delta_{j \leqslant \mathcal{L}_N(m)} \binom{\mathcal{L}_N(m)}{j} \omega^\beta(m) \times \sum_{x=1}^{2\mathfrak{f}_\chi} a_x(\chi) \cdot \delta_{\theta_N} \right) \bmod \mathcal{J}_N. \end{aligned}$$

Lastly we make an optimal choice of t under the constraint $N \leqslant t\phi(2\mathfrak{f}_\chi)$: that is, $t = \lfloor N/\phi(2\mathfrak{f}_\chi)\rfloor + 1$. The coefficient of X^j in the above coincides with that in equation (2), so the proof is complete. □

3. *An application to cubic fields*

From now on, suppose K is a cyclic cubic field of conductor $\mathfrak{f}$, with ring of integers $\mathcal{R}_K$ and discriminant $D_K = \mathfrak{f}^2$. Then K is necessarily totally real, and we write θ, θ' and θ'' for Gaussian periods associated to a generating cubic character $\chi : \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} \mu_3$, where μ_n denotes the nth roots of unity. In fact χ can be identified with an even Dirichlet character modulo $\mathfrak{f}$, and in Hasse's notation

$$\mathfrak{f} = \frac{a^2 + 3b^2}{4},$$

where the twin parameters $a, b \in \mathbb{Z}$ satisfy

$$\begin{cases} a \equiv 2 \bmod 3, b \equiv 0 \bmod 3, b > 0 & \text{if } 3 \nmid \mathfrak{f}, \\ a \equiv 6 \bmod 9, b \equiv 3 \text{ or } 6 \bmod 9, b > 0 & \text{if } 3 \mid \mathfrak{f}. \end{cases}$$

We begin by describing how to construct the values of each cubic character χ of conductor $\mathfrak{f}$.

3.1. *Generating the cubic character*

First, note that every cubic conductor has the special form $\mathfrak{f} = 3^{2e_3} \times \prod_{l \equiv 1 \bmod 3} l^{e_l}$, where the exponent $e_l \in \{0, 1\}$ for each prime l (since any cubic character trivialises on $\mathrm{Gal}(\mathbb{Q}(\mu_{l^\infty})/\mathbb{Q})$ if $l \equiv 2 \bmod 3$, and similarly trivialises on $\mathrm{Gal}(\mathbb{Q}(\mu_{l^\infty})/\mathbb{Q}(\mu_l))$ if the prime $l \neq 3$).

Let $\theta_l : \mathbb{F}_l^\times \to \mu_{l-1}$ denote the Teichmüller character modulo l, and write θ_9 for a non-trivial character modulo 9 such that $\theta_9|_{\mathbb{F}_3^\times} = \mathbf{1}$. Then the function

$$\chi'(n) := \begin{cases} \theta_9(n)^{e_3} \times \prod_l \theta_l(n)^{(l-1)e_l/3} & \text{if } \gcd(n, \mathfrak{f}) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

yields an even cubic character of conductor $\mathfrak{f}$ taking values in the Eisenstein integers $\mathbb{Z}[e^{2\pi i/3}]$. It follows that the field cut out by this character, K' say, is a totally real cyclic extension of $\mathbb{Q}$ with discriminant $D_{K'} = \mathfrak{f}^2$.

Remarks. (i) Exactly 217 out of the 501 cyclic fields of discriminant $<10^7$ have no other associated non-conjugate cubic field so, for these specimens, we deduce that $\chi' \in \{\chi, \chi^{-1}\}$.

(ii) In the remaining 284 examples, there are eight groups (each containing four non-conjugate fields) sharing the same field discriminant per group, while the leftover 252 fields pair into precisely two non-conjugate cubic fields for a particular discriminant (see [**11**, Tables 2 and 4]).

(iii) To generate χ when there is more than one non-conjugate cubic fields, we can, instead, take a product of the Hilbert symbols $(n/(c + de^{2\pi i/3}))_3$ over choices of prime ideal $\langle c + de^{2\pi i/3}\rangle \in \mathrm{Spec}\ \mathbb{Z}[e^{2\pi i/3}]$ with $c^2 - cd + d^2 = l \equiv 1 \bmod 3$, although the code itself can be somewhat laborious to run.

3.2. *Computing the cyclotomic λ-invariant of K*

Since the Iwasawa Main Conjecture holds over the totally real field K by Wiles [**19**, Theorem 1.2], both the analytic and algebraic λ-invariants coincide. The former is the easiest to calculate. Recall that under the mapping $s \mapsto -\log_p(1 + X)/\log_p(1 + p)$, the χ-twisted p-adic L-function

transforms into an element $F_{\chi,\beta}(X) \in \mathcal{O}[\![X]\!]$, where, for any such cubic character χ, the coefficient ring $\mathcal{O} = \mathbb{Z}_p[\mu_3]$ is a complete discrete valuation ring (d.v.r.) with residue field $\mathbb{F}_q$, and order

$$q = \begin{cases} p & \text{if } p \equiv 1 \bmod 3, \\ p^2 & \text{if } p \equiv 2 \bmod 3. \end{cases}$$

As discussed previously, there is a Weierstrass decomposition

$$F_{\chi,\beta}(X) = \mathcal{U}(X) \times (X^\lambda + b_{\lambda-1}X^{\lambda-1} + \ldots + b_0),$$

where $\mathcal{U}(X) \in \mathcal{O}[\![X]\!]^\times$ is an invertible power series and each $|b_j|_p < 1$ is in the range $0 \leqslant j < \lambda$. By its very nature, the invariant λ counts (with multiplicity) the number of zeros of $F_{\chi,\beta}(X)$ on the open p-adic unit disk.

We prefer to work with the power series $\mathcal{F}_{\chi,\beta}(X)$, which is the transform of the 2-modified p-adic L-function $(2\omega^\beta(2)\langle 2\rangle^{-s} - 1) \times L_p(s, \chi\omega^{1+\beta})$. Then, for some $\mathcal{U}^\dagger(X) \in \mathcal{O}[\![X]\!]^\times$,

$$\mathcal{F}_{\chi,\beta}(X) = \mathcal{U}^\dagger(X) \times (X^\lambda + b_{\lambda-1}X^{\lambda-1} + \ldots + b_0) \times \begin{cases} \left(X + \dfrac{p}{1+p}\right) & \text{if } \beta \equiv -1 \bmod p-1, \\ 1 & \text{if } \beta \not\equiv -1 \bmod p-1. \end{cases}$$

The set of zeros for both power series are identical, except when $\beta \equiv -1 \bmod p-1$, in which case there is one extra zero for $\mathcal{F}_{\chi,\beta}(X)$ at $X = -p/(1+p)$.

Let $\lambda_p(\chi\omega^{1+\beta})$ denote the λ-invariant attached to the $\chi\omega^{1+\beta}$-twisted p-adic zeta function. There are two methods that we shall use to determine λ_5 and λ_7: the first is faster than the second but it relies on p not dividing $\mathfrak{f} \times \phi(\mathfrak{f})$, while the second method is slow but unconditional. Throughout, we have adopted the first method wherever possible, resorting to the second option only when the former cannot be applied directly.

First method: One begins by determining the coefficients of the p-adic power series $\mathcal{F}_{\chi,\beta}(X)$ for a fixed branch $\beta \in \{1, 3, \ldots, p-2\}$. Henceforth, assume that $p \neq 2$ satisfies $\gcd(p, \mathfrak{f}\phi(\mathfrak{f})) = 1$. Recall one has the Taylor series expansion

$$\mathcal{F}_{\chi,\beta}(X) = \sum_{j=0}^{\infty} c_j(\mathcal{F}_{\chi,\beta}) \cdot X^j,$$

with each coefficient $c_j(\mathcal{F}_{\chi,\beta}) = \lim_{N\to\infty} c_j^{(N)}(\mathcal{F}_{\chi,\beta})$, where the Cauchy sequence $\{c_j^{(N)}(\mathcal{F}_{\chi,\beta})\}_{N\geqslant 1}$ was given in equation (2) by the formula

$$c_j^{(N)}(\mathcal{F}_{\chi,\beta}) := \sum_{m=1,\, p\nmid m}^{p^N} \binom{\mathcal{L}_N(m)}{j} \omega^\beta(m) \times \sum_{x=1}^{2\mathfrak{f}_\chi} a_x(\chi) \cdot \delta_{\theta_N(x,m) < p^{\mathcal{T}\phi(2\mathfrak{f}_\chi) - 2\mathfrak{f}_\chi p^N \gamma_{N,\mathcal{T}}}}.$$

The values of the cubic character χ (generated via the method of the last section) then allow us to calculate every $a_x(\chi) = \zeta(0,\chi) + \sum_{j=1}^{x-1} \chi(j) - 2\sum_{j=1}^{\lfloor (x-1)/2 \rfloor} \chi(j)$ using $O(\mathfrak{f}_\chi)$-summations.

PROPOSITION 1. *If* $\operatorname{ord}_p(c_j^{(2)}(\mathcal{F}_{\chi,\beta})) = 0$ *for some* $j \leqslant p$, *then*

$$\lambda_p(\chi\omega^{1+\beta}) = \min\{j \geqslant 0 \mid \operatorname{ord}_p(c_j^{(2)}(\mathcal{F}_{\chi,\beta})) = 0\} - \begin{cases} 1 & \text{if } \beta \equiv -1 \bmod p-1, \\ 0 & \text{if } \beta \not\equiv -1 \bmod p-1. \end{cases}$$

Proof. Applying Theorem 1 with $N = 2$, there are congruences

$$\begin{aligned}\mathcal{F}_{\chi,\beta}(X) &\equiv \sum_{j=0}^{p^2} c_j^{(2)}(\mathcal{F}_{\chi,\beta}) \cdot X^j \bmod (X,p)(X^p,p)\cdot\mathcal{O}[\![X]\!] \\ &\equiv \sum_{j=0}^{p} \overline{c_j^{(2)}(\mathcal{F}_{\chi,\beta})} \cdot X^j \bmod X^{p+1}\cdot\mathbb{F}_q[\![X]\!],\end{aligned}$$

where the horizontal bar denotes the reduction modulo p map $\mathcal{O}[\![X]\!] \twoheadrightarrow (\mathcal{O}/p)[\![X]\!] \cong \mathbb{F}_q[\![X]\!]$. In particular, if $c_j^{(2)}(\mathcal{F}_{\chi,\beta})$ is a p-adic unit for some $j < p+1$, then, as the μ-invariant of $\mathcal{F}_{\chi,\beta}(X)$ vanishes by [7], the smallest such j must be the λ-invariant of $\mathcal{F}_{\chi,\beta}(X)$. Furthermore,

$$\lambda(\mathcal{F}_{\chi,\beta}) = \lambda_p(\chi\omega^{1+\beta}) + \lambda(2\omega^{\beta}(2)\langle 2\rangle^{-s} - 1) = \lambda_p(\chi\omega^{1+\beta}) + \begin{cases} 1 & \text{if } \beta \equiv -1 \bmod p-1, \\ 0 & \text{if } \beta \not\equiv -1 \bmod p-1, \end{cases}$$

and hence the result follows. □

There are two ways one can apply this proposition.

Firstly, suppose that we fix the character χ and allow p to vary over the set of prime numbers. Assuming that the λ-invariant is less than or equal to p, by the previous result, one computes $c_j^{(2)}(\mathcal{F}_{\chi,\beta})$ until one hits a value of j (namely, $j = \lambda_p(\chi\omega^{1+\beta})$) for which $c_j^{(2)}(\mathcal{F}_{\chi,\beta})$ is a p-adic unit; as each computation of $c_j^{(2)}(\mathcal{F}_{\chi,\beta})$ requires $O(p^2\log p)$ operations, by Corollary 1, the total needed to find the λ-invariant is at worst $O(p^3\log p)$.

Secondly, suppose that we fix the prime number p and allow the character χ to vary. Here the calculation of $\lambda_p(\chi\omega^{1+\beta})$ is dominated by the cost of producing the coefficients $a_x(\chi)$ for $x = 1,\ldots,2\mathfrak{f}_\chi$ every time we switch to a new character χ; the latter calculation requires us to compute the values of χ and hence $a_x(\chi)$, which is an expensive process of type $O(\mathfrak{f}_\chi)$. This compares unfavourably with calculating the classical L-values $\zeta(-k,\chi)$, which is $O(\mathfrak{f}_\chi^{1/2+\epsilon})$, so, in this scenario, it seems preferable to rely on existing transcendental methods.

(In her Waikato Masters thesis, Nof Alharbi has used our formulae to study the λ-invariant in a family of quadratic extensions $\mathbb{Q}(\sqrt{d})$, and has adapted Theorem 1 to compute zeros for those twists with $\lambda_p(\chi_d\omega^{1+\beta}) > 0$, thereby confirming the results in [6] by another means.)

Lastly, a new paper of Roblot [15] describes an explicit method for computing special values of Shintani p-adic L-functions over totally real number fields, by using the cone decomposition into partial zeta functions developed by Pi. Cassou-Noguès. It would be a worthwhile project to combine Roblot's methods with the Dirichlet series expansions (only found over $\mathbb{Q}$ thus far) from [2, 3], and, consequently, extend the algorithm presented here to the totally real case.

Second method: Here we need make no assumption whatsoever on the choice of prime $p \neq 2$. Let $B_{n,\chi\omega^{\beta-1}}$ denote the $\chi\omega^{\beta-1}$-twisted Bernoulli number of index n. Then the identity

$$\Omega_{\chi,\beta}(r) := L_p(-p^r,\chi\omega^{1+\beta}) = \iota_p\left(-(1-\chi\omega^{\beta-1}(p)p^{p^r})\cdot\frac{B_{1+p^r,\chi\omega^{\beta-1}}}{1+p^r}\right)$$

follows easily from the interpolation formula in equation (1). The cost of computing $\Omega_{\chi,\beta}(r)$ is governed by the cost of computing each $B_{1+p^r,\chi\omega^{\beta-1}}$, while the latter can be calculated using the well-known formula

$$B_{n,\chi\omega^{\beta-1}} = (\mathfrak{f}_{\chi\omega^{\beta-1}})^{n-1} \times \sum_{a=1}^{\mathfrak{f}_{\chi\omega^{\beta-1}}} \chi\omega^{\beta-1}(a) \times \sum_{i=0}^{n}\binom{n}{i} B_i\left(\frac{a}{\mathfrak{f}_{\chi\omega^{\beta-1}}}\right)^{n-i},$$

where $\mathfrak{f}_{\chi\omega^{\beta-1}}$ is the conductor of $\chi\omega^{\beta-1}$ viewed as a primitive Dirichlet character.

PROPOSITION 2. *By expanding* $F_{\chi,\beta}(X) = \sum_{j=0}^{\infty} c_j(F_{\chi,\beta}) \cdot X^j$, *for all integers* $t \geqslant 1$,

$$c_0(F_{\chi,\beta}) \equiv \Omega_{\chi,\beta}(t-1) \mod p^t, \quad c_1(F_{\chi,\beta}) \equiv \frac{\Omega_{\chi,\beta}(t-1) - \Omega_{\chi,\beta}(2t-1)}{(1+p)^{p^{t-1}} - 1} \mod p^t,$$

and

$$c_2(F_{\chi,\beta}) \equiv \frac{\Omega_{\chi,\beta}(t-1) - \Omega_{\chi,\beta}(3t-1)}{((1+p)^{p^{t-1}} - 1)^2} + \frac{\Omega_{\chi,\beta}(4t-1) - \Omega_{\chi,\beta}(2t-1)}{((1+p)^{p^{2t-1}} - 1)((1+p)^{p^{t-1}} - 1)} \mod p^t.$$

In particular, choosing t equal to one allows us to determine $c_0(F_{\chi,\beta}), c_1(F_{\chi,\beta})$ and $c_2(F_{\chi,\beta})$ modulo p from the terms $\Omega_{\chi,\beta}(0), \ldots, \Omega_{\chi,\beta}(3)$, so one can check whether $\lambda_p(\chi\omega^{1+\beta})$ is zero, one, two, or greater than or equal to three. Of course if the λ-invariant is greater than or equal to three, then more of these coefficients $c_j(F_{\chi,\beta})$ are required to calculate it exactly, which may become relatively expensive from a computational perspective. Consequently, we only use the second method in place of the first when p divides $\mathfrak{f}$.

Proof. Substituting $X = (1+p)^{p^{t-1}} - 1$ into the Taylor series for $F_{\chi,\beta}(X)$, clearly gives

$$\Omega_{\chi,\beta}(t-1) = c_0(F_{\chi,\beta}) + c_1(F_{\chi,\beta}) \cdot ((1+p)^{p^{t-1}} - 1) + c_2(F_{\chi,\beta}) \cdot ((1+p)^{p^{t-1}} - 1)^2 + \ldots$$

and $\mathrm{ord}_p((1+p)^{p^{t-1}} - 1) = t$ at positive integers t.

The congruences for $c_0(F_{\chi,\beta}), c_1(F_{\chi,\beta}), c_2(F_{\chi,\beta})$ now follow by reducing the above equation modulo p^t, modulo p^{2t} and modulo p^{3t}, respectively. □

3.3. *Locating the zeros of* $\mathbf{L}_p(s, \chi\omega^j)$

In the situation where $\lambda(\chi\omega^{1+\beta}) > 0$, we now consider the problem of determining the zeros of the associated $\chi\omega^{1+\beta}$-twisted p-adic L-function. Under the Mazur-Mellin transform, any such zero s_0 is mapped to the value $x_0 = (1+p)^{-s_0} - 1 \in p\mathbb{Z}_p$ which itself is a zero of $\mathcal{F}_{\chi,\beta}$. However, in general, there may exist zeros of $\mathcal{F}_{\chi,\beta}(X)$ which do not arise from the image of this transform (see [1, Theorems 4 and 5] or [6, § 3] for a nice discussion of this phenomenon).

QUESTION. Given that $\lambda(\chi\omega^{1+\beta}) > 0$, how can we determine where the zeros of $\mathcal{F}_{\chi,\beta}(X)$ lie?

To answer the above question, we first need to find the coefficients of the polynomial

$$X^\lambda + a_{\lambda-1}X^{\lambda-1} + \ldots + a_0$$

occurring in the Weierstrass decomposition of $\mathcal{F}_{\chi,\beta}$; assume we want them modulo p^k, say. Note that the approach of Ellenberg, Jain and Venkatesh [4, Proposition 5.3] implies that if one knows the coefficients $c_j(\mathcal{F}_{\chi,\beta})$ of the power series $\mathcal{F}_{\chi,\beta}(X)$ up to an accuracy of p^{K+1-j}, then one can compute the first few coefficients $a_0, a_1, \ldots, a_{K-\lambda k}$ of its distinguished polynomial modulo p^k. Therefore, choosing the auxiliary integer K so that $k \leqslant \lfloor K/\lambda \rfloor$ ensures that $K - \lambda k \geqslant \lambda - 1$, and hence the entire collection of coefficients $a_0, a_1, \ldots, a_{\lambda-1}$ is found modulo p^k. Lastly, provided that the total number of zeros $\lambda(\mathcal{F}_{\chi,\beta})$ is less than or equal to four, the location of each zero can then be established using the classical formulae.

We should also point out that the formula given in Theorem 1 for the $c_j(\mathcal{F}_{\chi,\beta})$ required $p \neq 2$ to be coprime to $\mathfrak{f} \times \phi(\mathfrak{f})$. To our great surprise, we discovered that the formula for these approximations continued to hold true even without restricting p, in all the cases that we tried. This indicates that the first named author was over-zealous in the conditions imposed in [3], and so these formulae are likewise valid in the case where $p \mid \phi(\mathfrak{f})$ with $p \nmid 2\mathfrak{f}$.

That leaves us to deal with the situation where $p \mid \mathfrak{f}$. As we are considering only $p = 5$ and $p = 7$, the prime number 5 is automatically excluded, since none of the cubic conductors $\mathfrak{f}$ is divisible by 5. Therefore, let us suppose that $p = 7$ and put $\pi_7^+ := e^{2\pi i/7} + e^{-2\pi i/7}$, which generates $\mathbb{Q}(\mu_7)^+$. Here the character χ associated to the cubic field K is such that $\chi = \omega^{2m}\widetilde{\chi}$ for some integer $m \not\equiv 0 \pmod 3$ and cubic character $\widetilde{\chi}$ of conductor $\mathfrak{f}_{\widetilde{\chi}} = \mathfrak{f}/7$; one then has an isomorphism $K(\pi_7^+) \cong \widetilde{K}(\pi_7^+)$, where $\widetilde{K}$ denotes the real cubic field of discriminant $\mathfrak{f}_{\widetilde{\chi}}^2 = \mathfrak{f}^2/49$ cut out by $\widetilde{\chi}$. It follows that $\mathcal{F}_{\chi,\beta}(X) = \mathcal{F}_{\widetilde{\chi},\beta+2m}(X)$, and it is straightforward to work out the latter's zeros using Theorem 1 (as discussed above), because the prime number 7 does not divide $\mathfrak{f}_{\widetilde{\chi}}$.

3.4. *Determining the class number of $K(\mu_p)$*

Let us write $\mathrm{Irr}(\theta, \mathbb{Q}) = x^3 - Ax^2 + Bx - C$ for the minimal polynomial of three Gaussian periods θ, θ' and θ'' associated to a generating cubic character χ of K, taken with an appropriate sign. In particular, one has $A = \mathrm{Tr}(\theta) = \theta + \theta' + \theta''$, $B = \theta\theta' + \theta\theta'' + \theta'\theta''$ and $C = \mathrm{Norm}(\theta) = \theta\theta'\theta''$. Then $K = \mathbb{Q}(\theta)$ and

$$\mathrm{Irr}(\theta, \mathbb{Q}) = \begin{cases} x^3 + x^2 + ((1 - \mathfrak{f})/3)x + (\mathfrak{f}(a - 3) + 1)/27 & \text{if } 3 \nmid \mathfrak{f}, \\ x^3 - (\mathfrak{f}/3)x - \mathfrak{f}a/27 & \text{if } 3 \mid \mathfrak{f}, \end{cases}$$

where, as before, $\mathfrak{f} = (a^2 + 3b^2)/4$. A proof of this formula is given by Mäki in [**12**, pp. 7–9].

Remark. We wish to compute the class group of $K(\mu_p)$: in order to implement this into PARI, one needs to find an irreducible polynomial of degree $3(p-1)$ whose roots generate this field. Note that, although $\mathrm{Irr}(\theta, \mathbb{Q}) \times (x^p - 1)$ generates the number field, it is **not** irreducible.

Definition 2. For each prime p, one defines the monic polynomial $P_p(x) \in \mathbb{Z}[x]$ by

$$P_p(x) := (x^p - (\theta)^p) \times (x^p - (\theta')^p) \times (x^p - (\theta'')^p),$$

the roots of which are precisely $\{(e^{2\pi i/p})^j \cdot \theta,\ (e^{2\pi i/p})^j \cdot \theta',\ (e^{2\pi i/p})^j \cdot \theta''$ with $j = 0, \ldots, p-1\}$.

It follows, from this description of its roots, that the splitting field of $P_p(x)$ is equal to $\mathbb{Q}(\theta, \mu_p)$. Furthermore, we observe that $\mathrm{Irr}(\theta, \mathbb{Q}) = (x - \theta)(x - \theta')(x - \theta'')$ naturally divides into $P_p(x)$; in fact, the quotient polynomial

$$P_p^\dagger(x) := \frac{P_p(x)}{\mathrm{Irr}(\theta, \mathbb{Q})}$$

must be irreducible over $\mathbb{Q}$, since each of its roots generates $\mathbb{Q}(\theta, \mu_p)$ and $P_p^\dagger$ has the same degree as $[K(\mu_p) : \mathbb{Q}] = 3(p-1)$. For the primes $p = 5$ and $p = 7$, the numerator P_p of $P_p^\dagger$ can be explicitly determined as follows.

Lemma 1. (i) *If $p = 5$, then*

$$P_5(x) = x^{15} - \mathcal{A}_5 x^{10} + \mathcal{B}_5 x^5 - \mathcal{C}_5,$$

where

$$\begin{aligned} \mathcal{A}_5 &= A^5 - 5A^3B + 5A^2C + 5AB^2 - 5BC, \\ \mathcal{B}_5 &= B^5 - 5AB^3C + 5B^2C^2 + 5A^2BC^2 - 5AC^3, \\ \mathcal{C}_5 &= C^5. \end{aligned}$$

(ii) *If* $p = 7$, *then*

$$P_7(x) = x^{21} - \mathcal{A}_7 x^{14} + \mathcal{B}_7 x^7 - \mathcal{C}_7,$$

where

$$\begin{aligned}
\mathcal{A}_7 &= A^7 - 7A^5B + 7A^4C + 14A^3B^2 - 21A^2BC - 7AB^3 + 7AC^2 + 7B^2C,\\
\mathcal{B}_7 &= B^7 - 7AB^5C + 7B^4C^2 + 14A^2B^3C^2 - 21AB^2C^3 - 7A^3BC^3 + 7BC^4 + 7A^2C^4,\\
\mathcal{C}_7 &= C^7.
\end{aligned}$$

Proof. For each prime p and scalars $\alpha, \beta, \gamma \in \mathbb{C}$, consider the polynomial expansion

$$(x^p - \alpha^p)(x^p - \beta^p)(x^p - \gamma^p) = x^{3p} - (\alpha^p + \beta^p + \gamma^p)x^{2p} + (\alpha^p\beta^p + \alpha^p\gamma^p + \beta^p\gamma^p)x^p - (\alpha\beta\gamma)^p.$$

Taking $p = 5$ and $(\alpha, \beta, \gamma) = (\theta, \theta', \theta'')$, assertion (i) follows from the identities

$$\begin{aligned}
\alpha^5 + \beta^5 + \gamma^5 = {} & (\alpha+\beta+\gamma)^5 - 5(\alpha+\beta+\gamma)^3(\alpha\beta+\alpha\gamma+\beta\gamma) + 5(\alpha+\beta+\gamma)^2(\alpha\beta\gamma)\\
& + 5(\alpha+\beta+\gamma)(\alpha\beta+\alpha\gamma+\beta\gamma)^2 - 5(\alpha\beta+\alpha\gamma+\beta\gamma)(\alpha\beta\gamma)
\end{aligned}$$

and

$$\begin{aligned}
\alpha^5\beta^5 + \alpha^5\gamma^5 + \beta^5\gamma^5 = {} & (\alpha\beta+\alpha\gamma+\beta\gamma)^5 - 5(\alpha+\beta+\gamma)(\alpha\beta+\alpha\gamma+\beta\gamma)^3(\alpha\beta\gamma)\\
& + 5(\alpha\beta+\alpha\gamma+\beta\gamma)^2(\alpha\beta\gamma)^2 + 5(\alpha+\beta+\gamma)^2(\alpha\beta+\alpha\gamma+\beta\gamma)(\alpha\beta\gamma)^2\\
& - 5(\alpha+\beta+\gamma)(\alpha\beta\gamma)^3.
\end{aligned}$$

Similarly, if $p = 7$ and $(\alpha, \beta, \gamma) = (\theta, \theta', \theta'')$ again, then (ii) follows from the identities

$$\begin{aligned}
\alpha^7 + \beta^7 + \gamma^7 = {} & (\alpha+\beta+\gamma)^7 - 7(\alpha+\beta+\gamma)^5(\alpha\beta+\alpha\gamma+\beta\gamma) + 7(\alpha+\beta+\gamma)^4(\alpha\beta\gamma)\\
& + 14(\alpha+\beta+\gamma)^3(\alpha\beta+\alpha\gamma+\beta\gamma)^2 - 21(\alpha+\beta+\gamma)^2(\alpha\beta+\alpha\gamma+\beta\gamma)(\alpha\beta\gamma)\\
& - 7(\alpha+\beta+\gamma)(\alpha\beta+\alpha\gamma+\beta\gamma)^3 + 7(\alpha+\beta+\gamma)(\alpha\beta\gamma)^2\\
& + 7(\alpha\beta+\alpha\gamma+\beta\gamma)^2(\alpha\beta\gamma)
\end{aligned}$$

and

$$\begin{aligned}
\alpha^7\beta^7 + \alpha^7\gamma^7 + \beta^7\gamma^7 = {} & (\alpha\beta+\alpha\gamma+\beta\gamma)^7 - 7(\alpha+\beta+\gamma)(\alpha\beta+\alpha\gamma+\beta\gamma)^5(\alpha\beta\gamma)\\
& + 7(\alpha\beta+\alpha\gamma+\beta\gamma)^4(\alpha\beta\gamma)^2 + 14(\alpha+\beta+\gamma)^2(\alpha\beta+\alpha\gamma+\beta\gamma)^3(\alpha\beta\gamma)^2\\
& - 21(\alpha+\beta+\gamma)(\alpha\beta+\alpha\gamma+\beta\gamma)^2(\alpha\beta\gamma)^3\\
& - 7(\alpha+\beta+\gamma)^3(\alpha\beta+\alpha\gamma+\beta\gamma)(\alpha\beta\gamma)^3\\
& + 7(\alpha\beta+\alpha\gamma+\beta\gamma)(\alpha\beta\gamma)^4 + 7(\alpha+\beta+\gamma)^2(\alpha\beta\gamma)^4.
\end{aligned}$$

These equations can either be checked by hand(!), or by using a symbolic algebra package. □

The coefficients of $P_p(x)$, and hence of $P_p^\dagger(x)$, can now be calculated for both $p = 5$ and 7. Because $P_p^\dagger(x)$ is irreducible, there exists an isomorphism $K(\mu_p) \cong \mathbb{Q}[x]/\langle P_p^\dagger(x)\rangle$ of algebraic field extensions of degree $3p - 3$ over $\mathbb{Q}$. Lastly, the PARI/GP [14] command *bnfinit.clgp.no* works out the class number associated to the quotient polynomial $P_p^\dagger(x)$, under the default assumption that the generalised Riemann hypothesis (GRH) holds.

4. *Analysis of the results*

Looking through the Tables 1–3 of λ-invariants computed in the Appendix, we did not find a single invariant $\lambda_5(\chi\omega^{1+\beta})$ which was greater than one. However, this was not the case for

$p = 7$; in fact we found four occurrences (at $\mathfrak{f} = 547, 549, 2223$ and 2493) where $\lambda_7(\chi\omega^{1+\beta}) = 3$, and 27 examples with $\lambda_7(\chi\omega^{1+\beta}) = 2$. The precise distribution of these λ-invariants is given in Tables I and II below.

Without reading too much into such a small sample, it would suggest that approximately 4% of cubic 5-adic λ-invariants are positive, while roughly 13% of 7-adic λ-invariants are positive. Another observation is that up to discriminant $D_K < 10^7$, the equivalence

$$\text{`}\lambda_5(\chi\omega^{1+\beta}) \geqslant 1 \textit{ for some } \beta \in \{1,3\} \iff 5 \textit{ divides the class number of } K(\mu_5)\text{'}$$

holds for these cyclic cubic fields K. Similarly, the implication

$$\text{`}\lambda_7(\chi\omega^{1+\beta}) \geqslant 1 \text{ for some } \beta \in \{1,3,5\} \implies 7 \text{ divides the class number of } K(\mu_7)\text{'}$$

holds true up to discriminant $D_K < 10^7$. However, the reverse implication turns out to be false. To further the discussion, consider from [**18**, Theorem 4.17] the relative class number formula

$$\begin{aligned}\frac{\#\mathrm{Pic}^0(\mathcal{R}_K[\mu_p])}{\#\mathrm{Pic}^0(\mathcal{R}_K[\mu_p]^+)} &= \mathcal{Q}\cdot \#K(\mu_p)^\times_{\mathrm{tors}} \times \prod_{\eta\in\{\mathbf{1},\chi,\chi^{-1}\}} \prod_{\substack{\beta=1,\\ \beta \text{ odd}}}^{p-2} \left(-\frac{1}{2}B_{1,\eta\omega^\beta}\right)\\ &= \frac{\mathcal{Q}\cdot \#K(\mu_p)^\times_{\mathrm{tors}}}{2^{[K(\mu_p):\mathbb{Q}]/2}} \times \prod_{\eta\in\{\mathbf{1},\chi,\chi^{-1}\}} \prod_{\substack{\beta=1,\\ \beta \text{ odd}}}^{p-2} L_p(0,\eta\omega^{1+\beta}),\end{aligned}$$

where the second line follows by applying the p-adic interpolation rule given in equation (1). One finds from [**18**, Theorem 4.12] that the index term $\mathcal{Q} \in \{1,2\}$, and, consequently,

$$\mathrm{ord}_p(\mathbf{h}_p) = \mathrm{ord}_p(\mathbf{h}_p^+) + 1 + \sum_{\beta \text{ odd}} (\mathrm{ord}_p(L_p(0,\omega^{1+\beta})) + 2\cdot \mathrm{ord}_p(L_p(0,\chi\omega^{1+\beta}))). \tag{6}$$

Here we have written $\mathbf{h}_p$ (respectively $\mathbf{h}_p^+$) to abbreviate $\#\mathrm{Pic}^0(\mathcal{R}_K[\mu_p])$ (respectively $\#\mathrm{Pic}^0(\mathcal{R}_K[\mu_p]^+)$).

TABLE I. *The number of cyclic cubic fields K of discriminant $D_K < 10^7$ with prescribed $\lambda_5(\eta)$.*

$p = 5$	$\eta = \chi\omega^2$	$\eta = \chi$
$\#K$ with $\lambda_5(\eta) = 0$	478	483
$\#K$ with $\lambda_5(\eta) = 1$	23	18
$\#K$ with $\lambda_5(\eta) = 2$	0	0
$\#K$ with $\lambda_5(\eta) = 3$	0	0
$\#K$ with $\lambda_5(\eta) \neq 0$	23	18

TABLE II. *The number of cyclic cubic fields K of discriminant $D_K < 10^7$ with prescribed $\lambda_7(\eta)$.*

$p = 7$	$\eta = \chi\omega^2$	$\eta = \chi\omega^4$	$\eta = \chi$
$\#K$ with $\lambda_7(\eta) = 0$	433	432	440
$\#K$ with $\lambda_7(\eta) = 1$	58	57	52
$\#K$ with $\lambda_7(\eta) = 2$	8	10	9
$\#K$ with $\lambda_7(\eta) = 3$	2	2	0
$\#K$ with $\lambda_7(\eta) \neq 0$	68	69	61

In particular, if either $\mathbf{h}_p^+$ is divisible by a power of p or $\sum_\beta \lambda_p(\chi\omega^{1+\beta})$ is strictly positive, then one might reasonably expect $\mathrm{ord}_p(\mathbf{h}_p)$ to be a positive integer as well, and *vice versa*. However, the statement '$p \mid \mathbf{h}_p \iff \lambda_p(\chi\omega^{1+\beta}) \geqslant 1$' does *not* follow from the equation (6). To date, the best result along these lines is the generalisation of Kummer's criterion to totally real fields given in [**8**, Theorem 1] and [**9**]; one may then use the list of class numbers $\mathbf{h}_5$, $\mathbf{h}_7$ compiled in Tables 1–3 in the appendix to determine whether the prime numbers 5 and 7 are regular/irregular over each cubic field.

The nature of the zeros of $L_p(s, \eta\omega^{1+\beta})$, themselves, has a controlling influence on the arithmetic of the cyclotomic $\mathbb{Z}_p$-extension of K. Let $\mathfrak{X}_{\infty,K} := \varprojlim_n \mathfrak{X}_{n,K}$, where $\mathfrak{X}_{n,K}$ denotes the p-Sylow subgroup of $\mathrm{Pic}^0(\mathcal{R}_K[\mu_{p^n}])$. Then $\mathfrak{X}_{\infty,K}$ has a natural action of the Lie group

$$\mathrm{Gal}(K(\mu_{p^\infty})/\mathbb{Q}) \cong C_3 \times \mathbb{F}_p^\times \times \Gamma \quad \text{with } \Gamma = 1 + p\mathbb{Z}_p,$$

which extends, by continuity, to an action of the whole Iwasawa algebra $\Lambda = \mathbb{Z}_p[\![\Gamma]\!][C_3 \times \mathbb{F}_p^\times]$. Note that $\mathbb{Z}_p[\![\Gamma]\!]$ is non-canonically isomorphic to the power series ring $\mathbb{Z}_p[\![X]\!]$ upon sending a topological generator γ_0 of Γ to the polynomial $X + 1$.

Remark. For those who are unfamiliar with these notions, an excellent introduction to the structure theory of Λ-modules, as well as to the Iwasawa Main Conjecture over the rationals, is to be found in Washington's book [**18**, Chapters 13 and 15].

Recall that a polynomial $f(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_0 \in \mathcal{O}[X]$ is called 'distinguished' if $|b_j|_p < 1$ for every $j \in \{0, \ldots, n-1\}$. As a consequence of Wiles' fundamental work [**19**], at each odd branch $\beta \in \{1, 3, \ldots, p-2\}$, the corresponding $(\chi\omega^\beta)^{-1}$-eigenspace in $\mathcal{O} \otimes_{\mathbb{Z}_p} \mathfrak{X}_{\infty,K}$ is a finitely-generated Λ-torsion module. Furthermore, there exists a pseudo-isomorphism

$$(\mathcal{O} \otimes_{\mathbb{Z}_p} \mathfrak{X}_{\infty,K})^{(\chi^{-1}\omega^{-\beta})} \xrightarrow{\mathrm{ps}\,\cong} \bigoplus_{j=1}^{t} \mathcal{O}[\![X]\!]/(f_j(X)^{e_j}),$$

where the distinguished polynomials $f_j(X) \in \mathcal{O}[X]$ satisfy $\prod_{j=1}^t f_j(X)^{e_j} = F_{\chi,\beta}(X)$, up to an element of $\mathcal{O}[\![X]\!]^\times$ (see [**19**, Theorem 1.2]).

Proposition 3. *If $p = 5$ or 7, and for every cyclic cubic field K of discriminant $D_K < 10^7$ and conductor $\mathfrak{f}$, then each $(\chi\omega^\beta)^{-1}$-eigenspace in $\mathcal{O} \otimes_{\mathbb{Z}_p} \mathfrak{X}_{\infty,K}$ has a monogenic Λ-module structure: that is there exists a pseudo-isomorphism*

$$(\mathcal{O} \otimes_{\mathbb{Z}_p} \mathfrak{X}_{\infty,K})^{(\chi^{-1}\omega^{-\beta})} \xrightarrow{\mathrm{ps}\,\cong} \mathcal{O}[\![X]\!]/(F_{\chi,\beta}(X)).$$

Proof. If $\lambda_p(\chi\omega^{1+\beta}) = 1$, there is nothing to prove as $F_{\chi,\beta}(X) = (\text{linear polynomial}) \times (\text{unit})$. Hence, without loss of generality, we may assume that $p = 7$, in which case $\mathcal{O} = \mathbb{Z}_7[\mu_3] = \mathbb{Z}_7$. If $\lambda_7(\chi\omega^{1+\beta}) = 2$, then 26 out of the 27 specimen fields from Table 5 in the Appendix satisfy

$$|x_1|_7 = 7^{-1/2}, \quad |x_2|_7 = 7^{-1/2} \quad \text{and} \quad |x_1 - x_2|_7 = 7^{-1/2},$$

where x_1, x_2 are the two zeros of the power series $F_{\chi,\beta}(X)$. In particular, the roots x_1, x_2 generate a ramified quadratic extension of $\mathbb{Q}_7$ and the associated distinguished polynomial is an irreducible quadratic: therefore $(\mathcal{O} \otimes_{\mathbb{Z}_7} \mathfrak{X}_{\infty,K})^{(\chi^{-1}\omega^{-\beta})}$ cannot be pseudo-isomorphic to $\mathbb{Z}_7[\![X]\!]/f_1(X) \oplus \mathbb{Z}_7[\![X]\!]/f_2(X)$, as the associated polynomial does not split.

The missing example with $\lambda_7(\chi\omega^{1+\beta}) = 2$ occurs when $\mathfrak{f} = 2263 = (95^2 + 3 \times 3^2)/4$ and $\beta = 5$; here the roots x_1, x_2 instead satisfy

$$x_1 = 2 \times 7 + O(7^2), \quad x_2 = 0 + O(7^2) \quad \text{and} \quad |x_1 - x_2|_7 = 7^{-1}.$$

Consequently, its distinguished quadratic polynomial becomes equal to X^2-14X inside $\mathbb{F}_7[X]$, which means that it must split over $\mathbb{Q}_7$, via Hensel's lemma. However, the ideals generated by $X-x_1$ and $X-x_2$ are coprime in $\mathbb{Z}_7[\![X]\!]$, and one concludes that

$$\frac{\mathbb{Z}_7[\![X]\!]}{\langle X-x_1\rangle}\oplus\frac{\mathbb{Z}_7[\![X]\!]}{\langle X-x_2\rangle}\overset{\text{ps}\,\cong}{\longrightarrow}\frac{\mathbb{Z}_7[\![X]\!]}{\langle (X-x_1)(X-x_2)\rangle}\quad\text{upon using [18, Lemma 13.8].}$$

Finally there are four specimens in Table 5 with $\lambda_7(\chi\omega^{1+\beta})=3$, namely $(\mathfrak{f},\beta)=(547,1)$, $(549,1)$, $(2223,3)$ and $(2493,3)$; their respective distinguished polynomials are

$$\begin{gathered}X^3+42X^2+7X+35\quad\text{up to } O(7^2),\\ X^3+0X^2+14X+7\quad\text{up to } O(7^2),\\ X^3+0X^2+35X+35\quad\text{up to } O(7^2),\\ X^3+28X^2+21X+28\quad\text{up to } O(7^2),\end{gathered}$$

all of which are Eisenstein (and thus irreducible) over $\mathbb{Q}_7$, so the proof is complete. □

The perceptive reader will have noticed that for the situation where $(p,\mathfrak{f},\beta)=(7,2263,5)$, in the Appendix, we computed $c_0(\mathcal{F}_{\chi,\beta}),\dots,c_j(\mathcal{F}_{\chi,\beta}),\dots,c_9(\mathcal{F}_{\chi,\beta})$ up to an accuracy $O(p^{10-j})$. We could, in principle, have undertaken this task for all the cubic fields treated in this paper, but it is both time consuming and ultimately unnecessary in order to deduce Λ-monogeneity. Note that obtaining the distinguished polynomial associated to $\mathcal{F}_{\chi,\beta}$ up to an accuracy $O(p^k)$ requires us to calculate the individual $c_j(\mathcal{F}_{\chi,\beta})$ to accuracy $O(p^{(\lambda+\delta_{\beta=-1})\times k+1-j})$, where we have set $\delta_{\beta=-1}=1$ or $\delta_{\beta=-1}=0$, depending on whether $\beta\equiv-1\pmod{p-1}$ or not.

Acknowledgements. The authors thank Nof Alharbi, whose numerous computations of zeros for quadratic twists convinced them that the method would extend to cyclic cubic extensions. They are also grateful to Heiko Knospe and Akshay Venkatesh for their helpful comments on computing zeta functions, and to the anonymous referee for their insight and suggestions. In the Appendix, we used the public domain PARI/GP program, developed by the computational group [14] at Université de Bordeaux I – the computer code used to construct these tables is freely available from the authors on request.

References

1. N. Childress and R. Gold, 'Zeros of p-adic L-functions', *Acta Arith.* 48 (1987) 63–71.
2. D. Delbourgo, 'A Dirichlet series expansion for the p-adic zeta function', *J. Aust. Math. Soc.* 81 (2006) 215–224.
3. D. Delbourgo, 'The convergence of Euler products over p-adic number fields', *Proc. Edinb. Math. Soc.* 52 (2009) 583–606.
4. J. Ellenberg, S. Jain and A. Venkatesh, 'Modelling λ-invariants by p-adic random matrices', *Commun. Pure Appl. Math.* 64 (2011) 1243–1262.
5. R. Ernvall and T. Metsänkylä, 'A method for computing the Iwasawa λ-invariant', *Math. Comp.* 49 (1987) 281–294.
6. R. Ernvall and T. Metsänkylä, 'Computation of the zeros of p-adic L-functions', *Math. Comp.* 58 (1992) 815–830.
7. B. Ferrero and L. Washington, 'The Iwasawa μ_p-invariant vanishes for abelian number fields', *Ann. of Math.* (2) 109 (1979) 377–395.
8. R. Greenberg, 'A generalization of Kummer's criterion', *Invent. Math.* 21 (1973) 247–254.
9. M. Kida, 'Kummer's criterion for totally real number fields', *Tokyo J. Math.* 14 (1991) 309–317.
10. T. Kubota and H. Leopoldt, 'Eine p-adische Theorie der Zetawerte, I: Einführung der p-adischen Dirichletschen L-Funktionen', *J. reine angew. Math.* 214 (1964) 328–339.
11. P. Llorente and J. Quer, 'On totally real cubic fields with discriminant $D<10^7$', *Math. Comp.* 50 (1988) 581–594.
12. S. Mäki, *The determination of units in real cyclic sextic fields*, Lecture Notes in Mathematics 797 (Springer-Verlag, Berlin and New York, 1980).

13. B. Mazur and A. Wiles, 'Class fields of abelian extensions of $\mathbb{Q}$', *Invent. Math.* 76 (1984) 179–330.
14. The PARI Group at Université de Bordeaux I, PARI/GP Version 2.7.0, 2014, available online from http://pari.math.u-bordeaux.fr/.
15. X.-F. Roblot, 'Computing p-adic L-functions of totally real number fields', *Math. Comp.* 84 (2015) 831–874.
16. S. Wagstaff Jr., 'Zeros of p-adic L-functions', *Math. Comp.* 29 (1975) 1138–1143.
17. S. Wagstaff Jr., 'Zeros of p-adic L-functions II', *Number theory related to Fermat's last theorem (Cambridge, Mass.* 1981*)*, Progress in Mathematics 26 (Birkhäuser, 1982) 297–308.
18. L. Washington, *Introduction to cyclotomic fields*, 2nd edn, Graduate Texts in Mathematics 83 (Springer, 1997).
19. A. Wiles, 'The Iwasawa conjecture for totally real fields', *Ann. of Math.* 131 (1990) no. 3, 493–540.

Daniel Delbourgo
Department of Mathematics
University of Waikato
Private Bag 3105
Hamilton
New Zealand
delbourg@waikato.ac.nz

Qin Chao
Department of Mathematics
University of Waikato
Private Bag 3105
Hamilton
New Zealand
qinchao@me.com